REMARKS

The examiner is thanked for the performance of a thorough search. In this reply, claims 1, 2, 13-18, and 21-22 are canceled; claims 3-5, 8, 9, 11, 12, 19, 20, and 23-27 are amended; and new claims 28-35 are introduced. Hence, claims 3-12, 19, 20, and 23-35 are pending in the application. The amendments to the claims as indicated herein do not add any new matter to this application. Furthermore, amendments made to the claims as indicated herein have been made to exclusively improve readability and clarity of the claims and not for the purpose of overcoming alleged prior art. Each issue raised in the Office Action mailed is addressed hereinafter.

I. ISSUES NOT RELATING TO PRIOR ART

A. ELECTION/RESTRICTIONS

Claims 13-17 are canceled as directed to non-elected subject matter.

B. DRAWINGS

The Office Action objected to FIG. 1A and requested a substitute drawing labeled "Prior Art." A proper substitute sheet is submitted herewith. Reconsideration of the objection is respectfully requested.

C. SPECIFICATION

The Office Action objected to the specification. Page 2 of this reply presents corrective amendments. Reconsideration is respectfully requested.

D. CLAIM REJECTIONS RELATING TO RECITATION OF USE AND INDEFINITENESS—35 U.S.C §§101, 112

Paragraph 8 asserts that claims 1, 12, 18, 19, and 20 recite a use but omits necessary steps involved in the method or process. Paragraph 9 of the Office Action rejects claims 1, 12, 18, 19, and 20 under 35 U.S.C. §101 as allegedly reciting a use without process steps. In view of the amended claims and the following remarks, the rejection is respectfully traversed.

In amended claim 3, which incorporates the subject matter of original claim 1, and in claims 18, 19, and 20, the recitations of forward security, without relying on a key management process, and infeasibility are omitted. In claim 12, the amended language makes clear that the subsequent steps are performed to achieve forward security and infeasibility. The specification details how particular steps achieve the results of forward security and infeasibility. A person of ordinary skill in the art, reading the claims in light of the detailed and precise specification, would readily understand how the claim features provide the results of the recitations of forward security and infeasibility. Further, the amended claims clearly recite specific process steps and therefore constitute a proper statutory process. Reconsideration of the rejection under §101 is respectfully requested.

Paragraphs 7, 8, and 10-13 of the Office Action reject claims 1-12 under 35 U.S.C. §112, second paragraph, as allegedly indefinite. In view of the amended claims and the following remarks, the rejection is respectfully traversed.

Paragraph 10 states a rejection of all of claims 1-12, but paragraphs 11-13 state specific issues only for claims 1, 12, 18, 19, 20. It is unclear whether the Office Action is actually rejecting any claims other than 1, 12, 18, 19, and 20, because no specific issues are raised for claims 2-11, and because claims 18-20 are outside the range of 1-12 stated in paragraph 10. Thus, Applicant has insufficient notice of any issues that may exist for any claim other than 1, 12, 18, 19 and 20. Applicant has addressed the specific issues raised in the Office Action for those claims, and believes that all claims now overcome the rejection. If other issues exist, clarification is requested in the next Office communication, which should be a non-final action in view of the lack of clarity in the present Office Action.

Regarding paragraph 11, the amended claims delete the term "secrecy" in favor of "security" and the latter term is now used consistently in the claims. Thus, all claims have proper antecedent basis.

Regarding paragraph 12, after amendment the term "computationally infeasible" appears only in claims 10, 12, 27, and 35. The Office Action asserts that the quoted term is relative and therefore indefinite. This is incorrect, because the meaning of infeasibility is given in the specification. At page 21, the specification states, "a random-access key updating function is defined such that any future key can be computed efficiently, but finding previous keys is computationally infeasible." Page 23 states, "The functions 814, 816, 818 operate on values in the stack 806 and provide all operations needed to provide a cipher with random-access key updating." Page 29 discusses in detail how particular aspects of an embodiment achieve infeasibility:

> ... no previous keys are computable using $f_0$ and $f_1$ given the current value of the state retained by the traversal algorithm. While a previous key would be computable using $f_0$ and/or $f_1$ given one of its ancestors or itself, in the approach herein, for each value $X$ stored on the stack by the Initialization, Seek, or Advance functions, no ancestor of $X$ is stored. Since the current key is merely the contents of the node identified in the top element of the stack, no ancestor of the current key is ever stored. The Advance function discards each key as it is used, so no previous key or any ancestors of a previous key are stored. Further, since an adversary $A$ cannot distinguish the function $f_0$ or $f_1$ from a random function in polynomial time, a cipher that uses the keys associated with the leaves of a key updating tree, from left to right, to encrypt a sequence of messages provides forward security.

Thus, the specification provides ample information teaching how to implement the claims in a manner that results in infeasibility as claimed. A person of ordinary skill in the art would have

had ample detail to determine the scope of the invention, and therefore the claims cannot be indefinite.

Regarding paragraph 13, although Applicants disagree with the rationale of the Office Action—the specification makes clear that forward security is best achieved within a cipher rather than using other key management processes—the issue raised in paragraph 13 is moot in view of the amendments.

Reconsideration and withdrawal of the rejections under 35 U.S.C. § 112 are respectfully requested.

## II. ISSUES RELATING TO PRIOR ART

### A. CLAIMS 1, 12, 18, 19, AND 20—BELLARE ET AL.

Claims 1, 12, 18, 19, and 20 are rejected under 35 U.S.C. § 102(b) as allegedly unpatentable over Bellare et al. The rejection is respectfully traversed.

A rejection under §102 is traversed if the claims recite one or more features, elements, steps or limitations that are not found in the cited reference. Stated another way, the cited reference must teach or disclose each and every feature of the claims, arranged as in the claims. *See Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983). The claims of the present application contain features not found in the reference, and therefore the rejection is overcome.

Each of the independent claims recites "creating and storing values in a memory that correspond to a logical tree, wherein the tree represents the keystream, wherein each leaf node of the tree represents a particular keystream segment associated with a discrete location in the keystream, and wherein an order of each leaf node in pre-order traversal of the tree corresponds to a sequential order of all keystream segments." Bellare et al. fails to teach or disclose the use of a tree that is structured in the preceding way to hold and represent a keystream. The

preceding feature was present in original claim 12, but is not addressed or even acknowledged in the Office Action—the feature is simply ignored. Thus, as to claim 12, the Office Action fails to present a *prima facie* case of anticipation.

Claims 1, 18, 19, and 20 further feature "creating and storing an ordered plurality of data elements ..."; "advancing to the updated key by outputting that particular keystream segment stored in a next data element ..."; and "seeking a future key without discarding the updated key by locating a highest internal node in the tree ..." Bellare et al. fails to teach or disclose any of the preceding features.

For all the foregoing reasons, Bellare et al. does not anticipate the subject matter of any of the claims. Reconsideration is respectfully requested.

B. CLAIMS 1-12 AND 18-27—DOUBLE PATENTING

At pp. 5-6 the Office Action rejects claims 1-12 and 18-27 for alleged double patenting, and contends that priority must be resolved. The rejection is respectfully traversed.

In the Office Action, paragraph 17, page 5, refers to "claim 1-2," but paragraph 18 refers to claims 1-12. Applicants have assumed the Office Action intended to refer to claims 1-12 in all cases.

As quoted in the Office Action at paragraph 16, a statutory "same invention" double patenting rejection is proper only when a patent and an application are for "an invention **drawn to identical subject matter**." In practical application, if the claims of the patent and the application differ such that an embodiment falls within the scope of a claim in the application, but not the patent, then no double patenting rejection can be made. *See* MPEP 804(II)(A). The issue is whether the same invention is being claimed twice. *Id.* If the claims do not cover identical subject matter, then an obviousness-type double patenting rejection might be

appropriate, but a "same invention" type of rejection is not. Further, a statutory double patenting rejection is avoided if claims are not "coextensive in scope." MPEP 804.02(I).

The claims of the present application and the claims of the '354 patent are not identical. Therefore, the "same invention" statutory double patenting rejection is improper, and should be withdrawn. For example, claim 1 of the '354 patent recites "creating and storing a state value for a leaf node of a balanced binary tree, wherein the leaves of the tree represent the complete keystream and the leaf node represents the keystream segment at the location, by a preorder traversal of the tree from root node to the leaf node wherein a leftward tree branch transition comprises computing a first non-linear function and a rightward tree branch transition comprises computing a second non-linear function." The claims of the present application have no such limitations. Numerous other examples are readily apparent from the 62 claims of the '354 patent, and Applicants will not attempt to list all of them. As representative examples, claims 9, 10, 13, 27, and 42 of the '354 patent each recite particular mathematical relationships or computational steps that are not found in any claim of the present application. Therefore, the claims of the present application are not claiming the same invention as in the '354 patent, and a statutory double patenting rejection is unsupported in the record.

Comparing the claims in the converse direction, other differences are readily apparent. For example, all independent claims of the present application recite that key generation is performed "with forward security," and "determining another key value based on the current key, the updated key, and state values that are stored during the generating is computationally infeasible." All dependent claims incorporate these features by dependency. Even if the quoted features have no patentable weight with respect to prior art and even if the quoted limitations are indefinite—as asserted elsewhere in the Office Action, but denied by Applicants—the quoted

limitations make the plain language of the claims different from the claims of the '354 patent for the purposes of evaluating double patenting.

Each of the independent claims recites "creating and storing values in a memory that correspond to a logical tree, wherein the tree represents the keystream, wherein each leaf node of the tree represents a particular keystream segment associated with a discrete location in the keystream, and wherein an order of each leaf node in pre-order traversal of the tree corresponds to a sequential order of all keystream segments." Claims 1, 18, 19, and 20 further feature "creating and storing an ordered plurality of data elements ..."; "advancing to the updated key by outputting that particular keystream segment stored in a next data element ..."; and "seeking a future key without discarding the updated key by locating a highest internal node in the tree ..." The '354 patent does not claim any of the foregoing features.

Further, claim 12 contains 46 lines of text reciting numerous particular features that are found in none of the claims of the '354 patent—e.g., selecting a highest-ordered element; applying first and second pseudo-random functions to generate key values; identifying an internal node having a highest node number that is an ancestor of a first node. No reasonable comparison of claim 12 to the claims of the '354 patent can result in identifying any claim of the '354 patent that is identical to claim 12.

The Office Action makes no attempt to correlate any one claim of the '354 patent to any corresponding claim of the present application. (Indeed, while each of brackets 1 and 2 of MPEP Form Paragraph 8.34 calls for an Office Action to identify a claim in the singular and another single allegedly conflicting claim, the Office Action does not provide a claim-by-claim comparison or correlation.) In a case involving complex technical subject matter such as this, a broad assertion that 62 claims of a patent recite the same thing as the present application does not establish a rational basis for a double patenting rejection. The Office Action gives no

explanation and cites no legal authority for asserting a "same invention" statutory double patenting rejection when the claims of the patent and application are not identical. The Office has the burden of proof on all these issues, and the burden is not carried.

Because the double patenting rejection is not proper, the requirement for a priority assertion is incorrect. Reconsideration is respectfully requested.

III. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firm check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: February 15, 2006

/ChristopherJPalermo#42056/
Christopher J. Palermo
Reg. No. 42,056

2055 Gateway Place Suite 550
San Jose, California 95110-1093
Telephone No.: (408) 414-1080x202
Facsimile No.: (408) 414-1076